APPENDIX

Fraud Prevention Mechanisms for Cellular Telecommunications Networks

A Technical Analysis on behalf of Aurora Wireless Technologies Ltd.

Version 1.0
12 November 1999
CONFIDENTIAL

Atty. Dkt. 10942-025 9370
(AWT-002)

This page is blank intentionally and is included for pagination purposes only.

REVISION HISTORY

Date	Version	Author(s)	Reason for re-issu
12 Nov 1999	2.0	Mark Beckner	Revisions based on client comments.
25 Oct 1999	1.0	Mark Beckner	Revisions based on client comments.
13 Oct 1999	0.1	Mark Beckner	Initial draft provided for client review and comment regarding general content and structure.

This page is blank intentionally and is included for pagination purposes only.

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

LIST OF FIGURES

This page is blank intentionally and is included for pagination purposes only.

LIST OF TABLES

This page is blank intentionally and is included for pagination purposes only.

1 Introduction

1.1 Purpose & Scope

This document defines provides the results of a study undertaken on behalf of Aurora Wireless Technologies Ltd. to determine the feasibility of providing fraud prevention mechanisms within existing wireless network elements – e.g., mobile switching centers, visited location registers, home location registers, service control points, etc. Particular interest is given to describing the current and potential roles of a home location register in fraud prevention.

1.2 Document Overview

Section 2 provides an overview of the current cellular network architecture. The major network elements, their function and interfaces are introduced. This reference model is used in subsequent discussions of fraud prevention mechanisms

Section 3 briefly introduces the fraud prevention mechanisms that are in use. These mechanisms are profiling, personal identification numbers, radio frequency fingerprinting, roamer verification and reinstatement, authentication, and "intelligent" personal identification numbers.

A section is devoted to an in-depth look at each fraud prevention mechanism as to that mechanism's current implementation. If applicable, a roadmap is provided that details the requirements necessary to achieve implementation in a home location register.

- Section 4 discusses each fraud prevention mechanism in greater detail and provides the typical use of the mechanism.
- Section 5 outlines a hybrid mechanism that borrows the best traits of conventional fraud prevention technologies.

A summary section provides some insights in the form of contrasts and comparisons among the different fraud prevention mechanisms.

1.3 Conventions Used In This Document

Message sequence diagrams are used to describe message flows. In general, solid lines are used to denote well-known, even standard, protocols. Dashed lines denote protocols that are not yet well defined either because a standard does not exist or extensions to a base standard are required. Any specific conventions are listed in the introduction to each section as needed.

1.4 Terms, Acronyms, & Definitions

The following table provides a list of terms and acronyms used in this document and, where appropriate, a brief definition of the term or acronym.

AC	Authentication Center
ANL	Allowed Numbers List
BS	Base Station
CSR	Customer Service Representative
EIR	Equipment Identity Register
FE	Functional Entity
FP	Fraud Prevention
HLR	Home Location Register
IPIN	"Intelligent" PIN
IS41	Interim Standard 41. The MAP protocol used in North American cellular telecommunications networks.
ISDN	Integrated Services Digital Network
MAP	Mobile Application Part. A protocol standard for intersystem communications in wireless networks.
MC	Message Center
MDN	Mobile Directory Number
MS	Mobile Station
MSC	Mobile Switching Center. A serving MSC handles request for service from a mobile user; a gateway MSC directs calls to a mobile user.
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
RF	Radio Frequency
RFF	Radio frequency FingerPrinting
RVR	Roamer Verification and Reinstatement
SME	Short Message Entity
SPINA	Subscriber PIN Access
SPINI	Subscriber PIN Intercept
TTN	Transfer-To-Number
VC	Verification Center
VLR	Visited Location Register
VPC	Validation Processing Center

1.4.1 Selected IS41 Operations

The following lists common abbreviations for IS41 MAP operations:

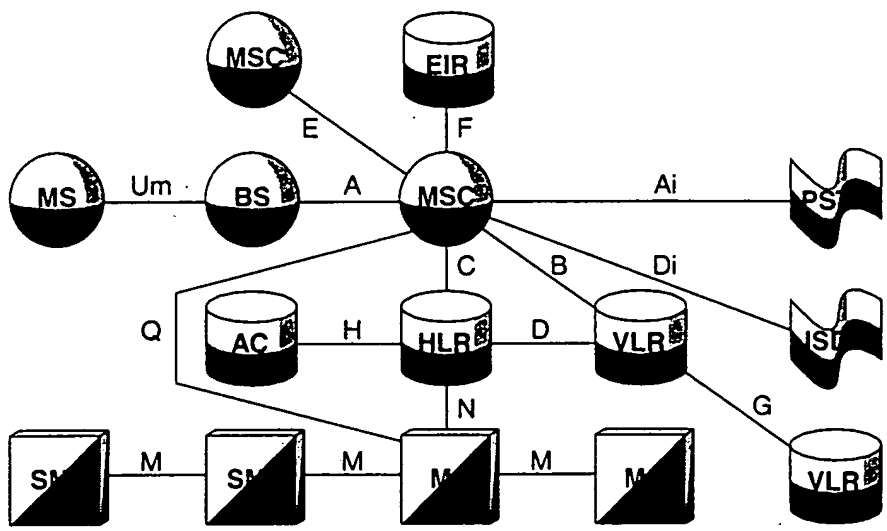
AUTHREQ	Authentication Request
AUTHREQ	Authentication Request
FEATREQ	Feature Request
ORREQ	Origination Request
REGCANC	Registration Cancellation
REGNOT	Regsitration Notification
RUIDIR	Remote User Interaction Directive

This page is blank intentionally and is included for pagination purposes only.

2 Network Architecture Reference Model

A cellular telecommunications network consists of a number of functional entities that interact across standard interfaces to provide a set of well-defined services. The network architecture reference model is shown in the figure below. In North America, IS41 defines the role of each functional entity and its interfaces.

Figure 2-1. Network Architecture Reference Model



Each of the line segments joining two functional entities represents a standard interface between those entities and is designated with a unique letter or letter sequence.

2.1 Functional Entities

2.1.1 Authentication Center

The AC is an entity that manages the authentication information related to a given MS. The AC may be co-located with the HLR FE in the same physical entity; however, an AC may serve more than one HLR.

2.1.2 Base Station

The BS is the site for all the radio equipment required for implementing one or several cells. It includes the sub-components of a base station controller and the base station receiver systems.

2.1.3 Equipment Identity Register

The EIR is the register or database to which user equipment identity may be assigned for record purposes. The EIR may be co-located with the MSC FE in the same physical entity.

2.1.4 Home Location Register

The HLR is the location register or database to which a user identity is assigned for record purposes such as subscriber information (e.g. ESN, DN, Profile Information, Current Location, and Authorization Period). The HLR may be co-located with the MSC FE in the same physical

entity; however, the HLR may serve more than one MSC and may be distributed over more than one physical entity.

2.1.5 Integrated Services Digital Network

The ISDN is a wide-area network that provides end-to-end digital transport and switching functions. It supports the carriage of traffic between mobile and non-mobile parties wishing to communicate.

2.1.6 Message Center

The MC is an entity that stores and forwards short messages. The MC may also provide supplementary services for Short Message Service.

2.1.7 Mobile Station

The MS is the interface equipment used to terminate the radio path at the user side. It provides the capabilities to access network services by the user.

2.1.8 Mobile Switching Center

The MSC is an automatic, system which constitutes the interface for user traffic between the cellular network and other public switched networks, or other MSCs in the same or other cellular networks.

2.1.9 Public Switched Telephone Network

The PSTN is a wide-area network that provides end-to-end transport and switching functions. It supports the carriage of traffic between mobile and non-mobile parties wishing to communicate.

2.1.10 Short Message Entity

The SME is an entity that composes and decomposes short messages. A SME may be co-located with an HLR, MC, VLR, MS, or MSC FE in the same physical entity.

2.1.11 Visited Location Register

The VLR is the location register or database other than an HLR used by an MSC to retrieve information for handling of calls to or from a visiting mobile user. The VLR may be co-located with an MSC FE in the same physical entity; however, the VLR may serve more than one MSC.

2.2 Interfaces

Each interface shown in the network architecture reference model represents a subset of the IS41 operations that comprise a cellular telecommunications network. Many of these interfaces are similar in that they support some of the same message sequences. However, they are not identical since each functional entity has unique responsibilities.

3 A Survey of Fraud Prevention Mechanisms

How can various FP mechanisms be compared? The 3 primary characteristics by which any FP mechanism can be measured are:

- **User convenience.** This is a measure of the degree of user involvement or impact that the FP mechanism requires. The more transparent the FP mechanism, the more convenient it is from the mobile user's perspective. From a service provider's perspective, convenience translates directly to customer satisfaction.

- **Prevention effectiveness.** The role of any FP mechanism is to prevent fraud; hence, a measure of effectiveness can be used to compare various approaches. Prevention effectiveness can have two components; *home market effectiveness* and *serving (roaming) market effectiveness.* Of these two components, serving market effectiveness is more important since roaming fraud represents hard monetary losses for the affected carrier. Fraud in the home market represents soft losses, mainly in terms of reduced capacity; capacity that could otherwise be used to serve legitimate, paying subscribers.

- **Cost efficiency.** Less expensive FP approaches are always better for any given level of prevention effectiveness. Any FP mechanism may require costs to be incurred by the deploying carrier, its roaming partners, its subscribers, or any combination of these three groups. A solution that limits expenditures to the deploying carrier is a better option when compared to another approach that has requires expenditures by roaming partners or subscribers.

These characteristics are presented above in an implied order of importance. User convenience outweighs prevention effectiveness and cost efficiency. Customers, typically unaware of or unconcerned about fraud, will desert their service provider for a more convenient form of service, given equal footing on price, coverage, etc., among competing service providers. Hence, carriers have learned not to choose FP solutions that present major inconvenience to their customers.

When the issue of user convenience is settled, prevention effectiveness has more weight than cost efficiency. Carriers will spend more to get a more effective FP solution. Often the choice of an FP approach is determined by a simple return-on-investment analysis.

3.1 First-Order Comparisons

With this in mind, the following subsections provide a brief overview of FP mechanisms and a first-order subjective rating against the comparison criteria described above. Our rating scale is from 1 to 5, lower numbers being better than higher numbers. The scale is applied as follows:

- User convenience. 1 - no impact will be detectable by the mobile user who perceives his/her service as unchanged; 2 - minor impact; 3 - moderate impact; 4 - major impact; 5 - extensive impact.

- Prevention effectiveness. 1 - the FP mechanism is extremely effective in both home and roaming markets; 2 - extreme effectiveness in roaming markets, but moderate effectiveness

in home markets; 3 - moderate effectiveness in both home and roaming markets; 4 - moderate effectiveness in home markets only; 5 - ineffective in home and serving markets.

- Cost efficiency. 1 - expenditures required by home carrier only; 2 - expenditures required primarily by home carrier and, to a lesser degree, roaming partners; 3 - expenditures required primarily by roaming partners and, to a lesser degree, the home carrier; 4 - some portion of the cost must be born by the subscriber; 5 - expenditure are required by the home carrier, its roaming partners, and its subscribers.

Weighting factors are applied for each criteria as follows:

- User convenience carries a weighting factor of 2.
- Prevention effectiveness carries a weighting factor of 1.5.
- Cost efficiency carries a weighting factor of 1.

Hence, the best FP approaches would have overall scores in the range 4.5-5.0. The worst approach would be rated 22.5.

3.1.1 Profiling

Profiling refers to the process of analyzing a mobile user's calling patterns after calls have occurred. It is more a fraud detection mechanism than a fraud prevention mechanism. It is included for completeness.

The purpose of profiling is primarily to identify cloning fraud in a billing stream for the purpose of removing fraudulent calls from the legitimate mobile user's billing records and preventing "sticker shock" when the monthly bill is received by the user.

Table 3-1. Profiling Subjective Rating

Criteria	Rating	Comments
Intrusiveness	1	Profiling totally non-intrusive since no user interaction is required.
Prevention Effectiveness	5	Profiling is not real-time; hence, it can not prevent fraud occurrences prior to calls being established.
Cost Efficiency	2	Profiling uses centralized shared systems; i.e., clearinghouse or service bureau model applies allowing costs to be amortized over a larger number of users. Roaming partners must re-configure their billing streams to feed the home carrier's profiling system.
Overall Rating	11.5	This is the weighted average of the above three ratings.

Profiling is one of the most mature fraud prevention mechanisms. It was developed with the express intent of not requiring access to either mobility management or call control signaling within a network. Hence, profiling, by design, is not suited to HLR implementation and will not be discussed further in this document.

3.1.2 Personal Identification Number

PINs are a simple means of identify a legitimate user prior to call establishment. On placing a call, the user is prompted to enter a PIN before the call can continue. A key assumption related to effectiveness is that only the legitimate user knows the correct PIN.

Table 3-2. PIN Subjectiv Rating

Criteria	Rating	Comments
Intrusiveness	4	PIN is inconvenient for legitimate users; it requires dialing extra digits on each call or purchasing a phone that can automatically dial a PIN.
Prevention Effectiveness	3	Effectiveness is poor since cloners can easily detect PINs for a given mobile user. PIN on all calls only helps the cloner achieve a high rate of successful compromises.
Cost Efficiency	3	This approach requires a PIN feature in each serving MSC and bi-lateral agreements with roaming partners to honor PINs.
Overall Rating	15.5	This is the weighted average of the above three ratings.

PIN is another mature FP mechanism. Sometimes referred to as "pre-call validation", two varieties of PIN have been developed and deployed; Subscriber PIN Access (SPINA, [spin´a]) and Subscriber PIN Intercept (SPINI, [spin´e]). Both require some portion of their functionality to be implemented in the HLR.

3.1.3 RF Fingerprinting

RFF is a process that validates the RF signature of a legitimate mobile user's handset prior to call establishment. A stored signature is compared to a signature captured in real-time. If the signatures are statistically similar, the call is allowed to complete.

Table 3-3. RF Fingerprinting Subjective Rating

Criteria	Rating	Comments
Intrusiveness	2	Althought no interaction with a mobile user is required with this approach, a measurable number of false positive determinations will cause legitimate calls to be incorrectly denied.
Prevention Effectiveness	3	This approach requires a large signature sample set to achieve necessary accuracy in identifying legitimate handsets.
Cost Efficiency	3	RF fingerprinting requires hardware installed at each base station site in home and roaming networks where signature capture is desired. In addition dedicated facilities are needed to connect base station equipment to a centralized site.
Overall Rating	11.5	This is the weighted average of the above three ratings.

RF fingerprinting requires that the BS equipment detecting a handset signature or fingerprint be able to communicate with a centralized fingerprint database for updating collected signatures or accessing stored signatures for comparison. Such database functionality could easily reside in an HLR.

A major roadblock to co-locating the RFF database with the HLR is the fact that the network reference model does not currently support a BS-to-HLR interface. As a result, RFF vendors have developed proprietary BS-to-RFF database interfaces; thus, the RFF database is not well suited to HLR implementation. RFF will not be discussed further in this document.

3.1.4 Roamer Verification & Reinstatement

RVR validates a roamer's identity as they register within a visited serving market. Registration events are captured by the RVR system and a customer service representative places a call to the roaming mobile user. A verbal challenge must be correctly answered for the roaming user to be registered in the serving market.

Table 3-4. RVR Subjective Rating

Criteria	Rating	Comments
Intrusiveness	3	The mobile user is required to answer a challenge before receiving service in the roaming service area.
Prevention Effectiveness	3	RVR makes it difficult for a cloner to answer the verbal challenges, which are a set of highly personal questions that are tailored to the individual mobile user. However, when a mobile has been authenticated in a serving market, there is a risk of cloning fraud during the time that the mobile registration is allowed.
Cost Efficiency	1	RVR only requires hardware installed at the HLR(s) within the home market. No special action is required on the part of subscribers or roaming partners to implement RVR.
Overall Rating	11.5	This is the weighted average of the above three ratings.

Portions of RVR functionality may be appropriate for HLR implementation since RVR is driven from the events and messages that are directed at an HLR. However, the challenge/response mechanism of RVR is not well suited to implementation in an HLR.

3.1.5 Authentication

RF fingerprinting is a process that validates the RF signature of a legitimate mobile user's handset prior to call establishment. A stored signature is compared to a signature captured in real-time. If the signatures are statistically similar, the call is allowed to complete.

Tabl 3-5. Auth ntication Subj ctiv Rating

Criteria	Rating	Comments
Intrusiveness	4	Authentication requires the mobile user to upgrade his/her handset.
Prevention Effectiveness	1	Cryptographic techniques provide pre-call authentication and excellent security for in-call bearer information (e.g., voice or data). For the carrier, effectiveness is proportional to the percentage of the subscriber base that uses authentication-capable handsets.
Cost Efficiency	5	Although network equipment to support authentication is centralized and can be shared among carriers, authentication requires mobile handsets that implement authentication as well as support from roaming partners.
Overall Rating	14.5	This is the weighted average of the above three ratings.

Noting the adjacency of an AC and HLR in the network reference model, one would expect that these two functional entities are ideal for physical co-location. The HLR role as the data store for subscriber information supports a strong argument for a tight coupling of the AC and HLR functions.

3.1.6 "Intelligent" PIN

"Intelligent" PIN (IPIN) is a variation on personal identification numbers that couples PIN use with a called number profile that is unique to a given mobile user. A mobile user is prompted to enter a PIN only when a call is placed to a number that is not in the user's called number profile. Successful PIN entry causes the called number to be entered into the user's profile so that subsequent calls to the same number will not require a PIN entry.

Table 3-6. "Intelligent" PIN Subjective Rating

Criteria	Rating	Comments
Intrusiveness	2	The mobile user is required to enter a PIN only on calls to numbers that are not listed in his/her called number profile
Prevention Effectiveness	3	Reduced PIN use increases the difficulty of compromise. PIN compromise can be detected and the legitimate user prompted to change his/her PIN.
Cost Efficiency	3	IPIN requires software features to be enabled in both the home and each roaming market.
Overall Rating	11.5	This is the weighted average of the above three ratings.

As with the PIN variations, SPINA and SPINI, IPIN requires some of its functionality to be implemented in an HLR.

3.2 Side-by-Side Comparisons

Table 3-7. Comparative Ratings

Evaluation Criteria	Profiling Rating	PIN Rating	RFF Rating	RVR Rating	Authentic. Rating	IPIN Rating
Intrusiveness	1	4	2	3	4	2
Prevention Effectiveness	5	3	3	3	1	3
Cost Efficiency	2	3	3	1	5	3
Overall Rating	11.5	15.5	11.5	11.5	14.5	11.5

4 Conventional Fraud Prevention Mechanisms Suitable to HLR Implementation

This section presents the FP technologies that are fit for implementation in an HLR or VLR. These are the three varieties of PIN – SPINA, SPINI, and IPIN – and Authentication, and RVR.

A critical aspect of any service implementation is the variations that may exist across different vendors' products. In the descriptions below, it is typically the case that one manufacturer will produce the MSC and VLR and a different manufacturer will produce the HLR. This situation gives rise to incompatible implementations of a given set of capabilities since not all aspects of the IS41 standard are required to be implemented.a

Conventions Used in This Section

In the following sections, IS41 operations sequences are diagramed. IS41 operations typically follow a remote procedure call model for distributed systems; i.e., each operation consists of an *invoke* message and an associated *response* message. By convention, an invoke message name is capitalized while the response message name is given in small letters.

The diagrams follow this convention as well as showing IS41 messages with solid arrows going from the sending FE to the receiving FE. Message contents are not formally listed, but the stereotypical use of the message is given by the phrase enclosed in guillemets (« »).

Dashed lines and message labels that are given with an initial capital letter indicate operations or messages that are not related to IS41 operations.

Processes or functions internal to a functional entity are shown as labeled rectangles with italicized labels. These functions represent significant functionality that must be implemented within the FE.

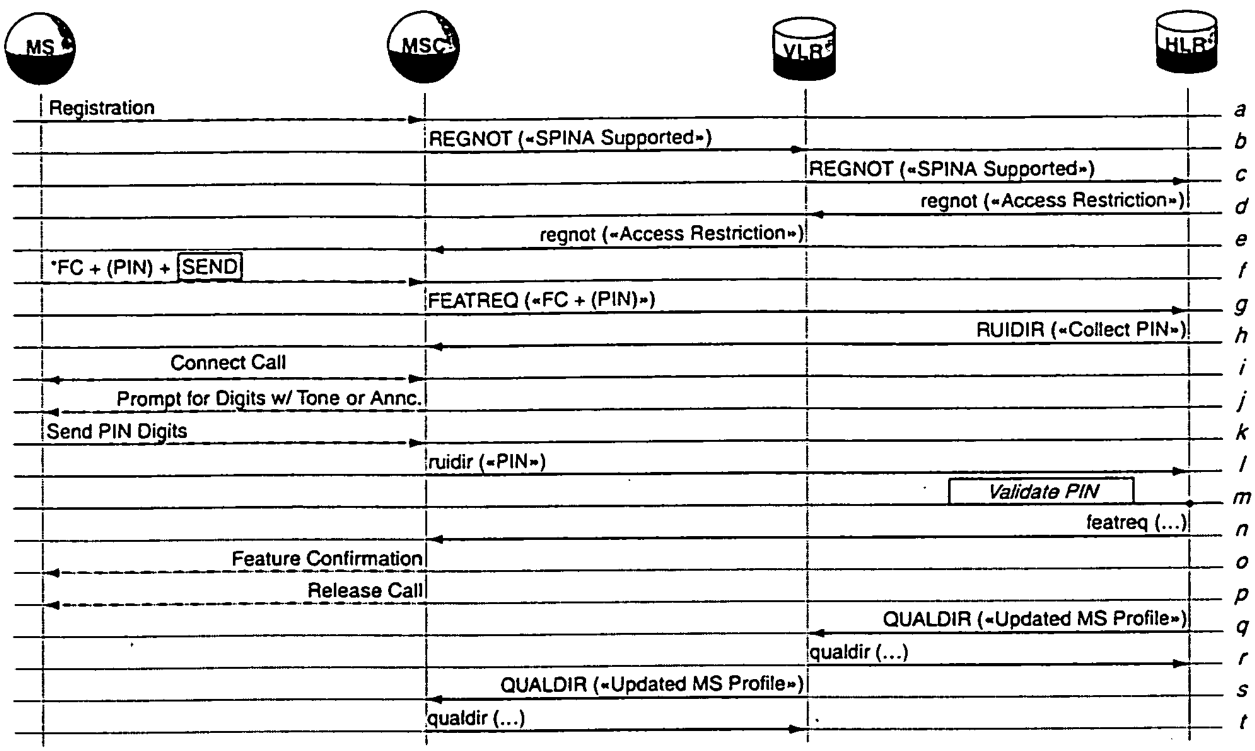
4.1 Personal Identification Number - SPINA Variation

SPINA allows a mobile user to enable and disable his/her service in a given serving (roaming) market. Once enabled, the mobile user may place calls without restriction. A weakness of this approach is that once enabled, the handset can be cloned and fraudulent usage accumulated against the account of the legitimate mobile user.

4.1.1 Architecture Overview

A operation sequence diagram is shown below for SPINA. Each step of the sequence is briefly described. Although many variations exist for this operational scenario, only the typical case is shown.

Figure 4-1. SPINA Architecture Model



a. A mobile user roams to a serving market where the SPINA feature is available.

b. A registration notification is sent from the MSC to the VLR. The REGNOT message indicates that the serving market supports SPINA.

c. The REGNOT is forwarded to the HLR.

d. The regnot response contains an access restriction on the mobile user such that calls may not be originated by nor terminated to the mobile user, which is enforced in normal operation of the MSC/VLR in the serving market.

e. The regnot response is forwarded to the serving MSC.

f. To enable service, the user dials a feature code (possibly concatenated with the user's PIN) to enable service in the serving area.

g. The FEATREQ message is sent to the HLR to request service activation in the serving market. If the PIN is provided, the scenario continues at step m.

h. If PIN is not provided in the FEATREQ message, using a RUIDIR message, the HLR may direct the serving MSC to collect a PIN from the mobile user.

i. The serving MSC connects a voice channel to the MS.

j. The user is prompted with a tone or announcement to enter the PIN.

k. The PIN is sent to the serving MSC.

l. The serving MSC returns the PIN to the HLR in the ruidir response message.

m. The HLR compares the PIN to a stored value for the mobile user.

n. If the entered and stored PINs match, the featreq response message indicates success to the serving MSC; otherwise, the response indicates failure.

o. The serving MSC plays a confirmation tone to the mobile user.

p. The call is released.

q. The HLR issues a QUALDIR message to the VLR with an updated profile that has the effect of removing the access restriction that were set in step d; e.g., the profile indicates that the mobile user is allowed to place and receive calls in the serving market.

r. The VLR acknowledges the QUALDIR message with a response.

s. In turn, the VLR updates the mobile user profile at the serving MSC.

t. The MSC acknowledges the QUALDIR message with a response.

If the PIN match fails, the HLR simply leaves the prior access restriction in place (i.e., omits steps p through s). A failure message or tone may be played to the mobile user.

4.1.2 Implementation Requirements

For the most part SPINA, is relatively simple to implement within the home and serving markets. A majority of the burden is on the home market.

4.1.2.1 Home Market Requirements

The HLR must implement the three IS41 operations required to implement SPINA -- FEATREQ, RUIDIR, QUALDIR. This typically means the HLR must have IS41 Revision C (or later) compliance to support the RUIDIR operation. An HLR implementing an earlier version of IS41 will have to be upgraded.

In addition, the HLR must implement the SPINA feature logic. This represents a departure from the HLR's role as a mobility or roaming management element. Hence, a specific vendor may require additional upgrades to their HLR product in order to accommodate this expanded role.

The mobile user database within the HLR has to be expanded to allow for PIN storage and administration in the HLR. This implies increased memory requirements in the HLR and changes to the database administration interface to perform add / modify / delete operations on a user record related to PIN administration (e.g., establishing, resetting, or removing the SPINA feature for an individual user).

4.1.2.2 Serving Market Requirements

The MSC in the serving market must be upgraded to IS41 Revision C capabilities to support the RUIDIR operation.

It is likely that the prompt for PIN digits, either a tone or announcement, pre-exists in the MSC; hence, no additional upgrades are likely to be required for this capability.

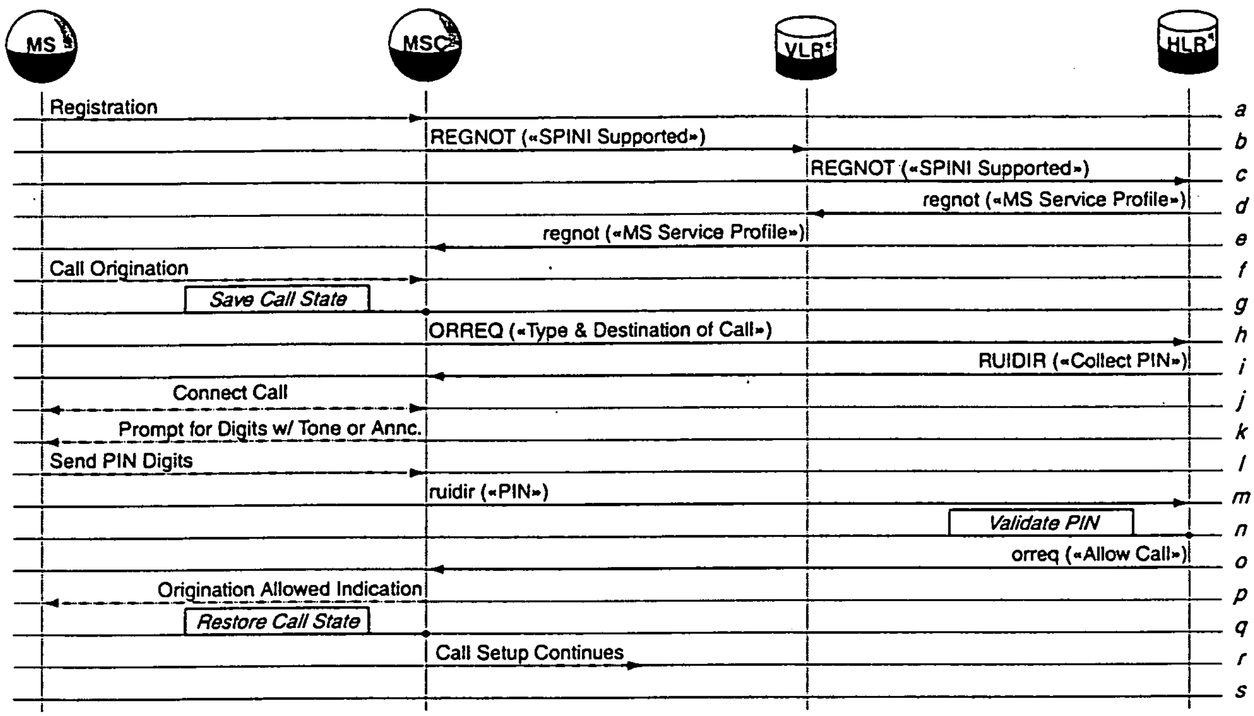
4.2 Personal Identification Number - SPINI Variation

SPINI is similar to SPINA with the exception that the mobile user must enter his/her PIN prior to every call placed by the user.

An origination request operation allows the serving system to report the details of the call origination – called number and type of call; e.g., local, long distance, etc. – to the HLR.

4.2.1 Architecture Overview

Figure 4-2. SPINI Architecture Model



a. A mobile user roams to a serving market where the SPINI feature is available.

b. A registration notification is sent from the MSC to the VLR. The REGNOT message indicates that the serving market supports SPINI.

c. The REGNOT is forwarded to the HLR.

d. The regnot response contains a service profile for the MS that indicates the type of calls for which an ORREQ operation should be initiated; e.g., local, long distance, etc.

e. The regnot response is forwarded to the serving MSC.

f. The mobile user dials a call in the normal fashion.

g. The serving determines that the SPINI feature is in effect for the MS and saves the call state.

h. The serving MSC sends an ORREQ message is sent to the HLR and indicates the called number and the type of call; e.g., local, long distance, international, etc..

i. Using a RUIDIR message, The HLR directs the serving MSC to collect a PIN from the mobile user.

j. The serving MSC connects a voice channel to the MS.

k. The user is prompted with a tone or announcement to enter the PIN.

l. The PIN is sent to the serving MSC.

m. The serving MSC returns the PIN to the HLR in the ruidir response message.

n. The HLR compares the PIN to a stored value for the mobile user.

o. The HLR compares the PIN to a stored value for the mobile user. If the entered and stored PINs match, the orreq response message indicates to the serving MSC that the call should be allowed

p. The serving MSC plays a confirmation tone to the mobile user.

q. The serving MSC restores the prior saved call state and continues with normal call processing.

r. The serving MSC routes the call to the original dialed number.

In the case that the PIN match fails, the HLR directs the serving MSC to disconnect the call. In which case, a failure message or tone may be given to the user.

4.2.2 Implementation Requirements

Compared to SPINA, there is an increased burden on implementation of SPINI in both the home and serving markets.

4.2.2.1 Home Market Requirements

The HLR must implement the two IS41 operations required to implement SPINI – ORREQ and RUIDIR. This typically means the HLR must have IS41 Revision C (or later) compliance to support these operations. An HLR implementing an earlier version of IS41 will have to be upgraded.

Similar to SPINA, the HLR must implement the SPINI feature logic. This represents a departure from the HLR's role as a mobility or roaming management element. Hence, a specific vendor may require additional upgrades to their HLR product in order to accommodate this expanded role.

The mobile user database within the HLR has to be expanded to allow for PIN storage and administration in the HLR. This implies increased memory requirements in the HLR and changes to the database administration interface to perform add / modify / delete operations on a user record related to PIN administration (e.g., establishing, resetting, or removing the SPINI feature for an individual user).

Another impact on the HLR is the increased processing workload due to the *per call* nature of the SPINI feature; every call origination requires HLR processing. As a result, the HLR may require significant hardware upgrade to handle this larger workload.

4.2.2.2 Serving Market Requirements

The MSC in the serving market must be upgraded to IS41 Revision C capabilities to support the ORREQ and RUIDIR operations.

It is likely that the prompt for PIN digits, either a tone or announcement, pre-exists in the MSC; hence, no additional upgrades are likely to be required for this capability.

The serving MSC also experiences an increased *per call* workload for each SPINI call that is placed. The normal call processing logic in the serving MSC has to be modified to allow HLR participation – i.e., the *Save Call State* and *Restore Call State* functionality. This may require significant software restructuring in the MSC such that the serving market operator may want the home market operator to bear some or all of the cost of implementing the feature.

4.3 Personal Identification Number - IPIN Variation

Similar to SPINI, IPIN provides a level of security against cloning fraud by requiring mobile user identification with a PIN for certain call originations.

In contrast to SPINI, the digit sequence dialed by the user to originate a call (i.e., the called number) is compared to a list of destinations that is specific to that user. This list is referred to as the user's *allowed destinations list* (ANL). If the called number is in the ANL, the call is allowed to complete without requiring a PIN entry. If the called number is not in the ANL, the user is prompted to enter a previously registered PIN. If the user correctly enters the PIN, the call origination is allowed and the called number is added to the user's ANL. On subsequent calls to the same called number, the user will not be prompted to enter a PIN. An invalid PIN entry, possibly after an optional number of retries, results in call denial treatment.

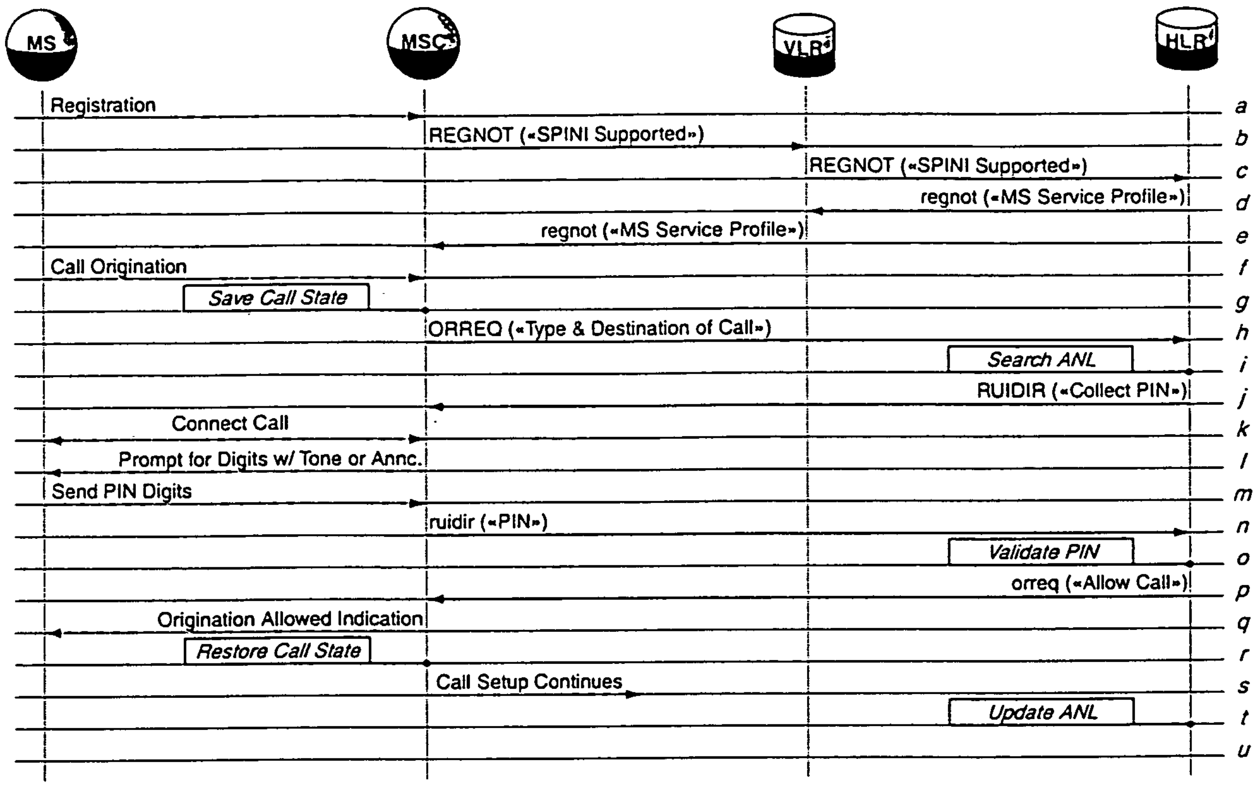
Assuming IPIN is invoked, there are several screening options available to the home market carrier:

- "Always Allow" called numbers – The carrier may specify a list of called numbers, common to all or a subset of the carrier's mobile users, that will never require a PIN. These called numbers, taken collectively, are referred to as *bypass numbers* or a *bypass list*; i.e., the PIN collection operation is bypassed for calls to these numbers.
- "Always Require PIN" Called Numbers – The carrier may specify a list of called numbers, common to all or a subset of the carrier's mobile users, that will always require a correct PIN entry.
- "Always Deny" Called Numbers – The carrier may specify a list of called numbers, common to all or a subset of the carrier's mobile users, that will always result in call denial treatment.

4.3.1 Architecture Overview

IPIN uses the same messaging sequences as SPINI. However, it does require increased functionality within the HLR.

Figure 4-3. IPIN Architecture Model



a. A mobile user roams to a serving market where the SPINI feature is available.

b. A registration notification is sent from the MSC to the VLR. The REGNOT message indicates that the serving market supports SPINI.

c. The REGNOT is forwarded to the HLR.

d. The regnot response contains a service profile for the MS that indicates the type of calls for which an ORREQ operation should be initiated.

e. The regnot response is forwarded to the serving MSC.

f. The mobile user dials a call in the normal fashion.

g. The serving determines that an ORREQ operation is required is in effect for the MS and saves the call state.

h. The serving MSC sends an ORREQ message is sent to the HLR and indicates the type of call (e.g., local, long distance, international, etc.).

i. The HLR searches the ANL for the mobile user to determine if the called number is in the list. If so, the sequence continues at step p.

j. Using a RUIDIR message, The HLR directs the serving MSC to collect a PIN from the mobile user.

k. The serving MSC connects a voice channel to the MS.

l. The user is prompted with a tone or announcement to enter the PIN.

m. The PIN is sent to the serving MSC.

n. The serving MSC returns the PIN to the HLR in the ruidir response message.

o. The HLR compares the PIN to a stored value for the mobile user.

p. The HLR compares the PIN to a stored value for the mobile user. If the entered and stored PINs match, the orreq response message indicates to the serving MSC that the call should be allowed

q. The serving MSC plays a confirmation tone to the mobile user.

r. The serving MSC restores the prior saved call state and continues with normal call processing.

s. The serving MSC routes the call to the original dialed number.

t. If the called number is not in the ANL, the HLR updates the list to include it. Subsequent calls to the number will not require a PIN collection operation.

In the case that the PIN match fails, the HLR directs the serving MSC to disconnect the call. In which case, a failure message or tone may be given to the user.

4.3.2 Implementation Requirements

4.3.2.1 Home Market Requirements

The home market requirements for IPIN are a superset of the requirements for SPINI described previously.

In addition to the required IS41 operations and SPINI functionality, the HLR must be modified to implement the ANL for each mobile user.

The mobile user database within the HLR has to be expanded to allow for ANL storage and administration in the HLR. This implies increased memory requirements in the HLR and changes to the database administration interface to perform add / modify / delete operations on a user record related to ANL administration (e.g., establishing, resetting, or removing the SPINI feature for an individual user).

Another impact on the HLR is the increased processing workload due to the *per call* nature of the IPIN feature; every call origination requires HLR processing to search and update the ANL. As a result, the HLR may require significant hardware upgrade to handle this larger workload.

4.3.2.2 Serving Market Requirements

The serving market requirements for IPIN are identical to those for SPINI described previously.

4.4 Authentication

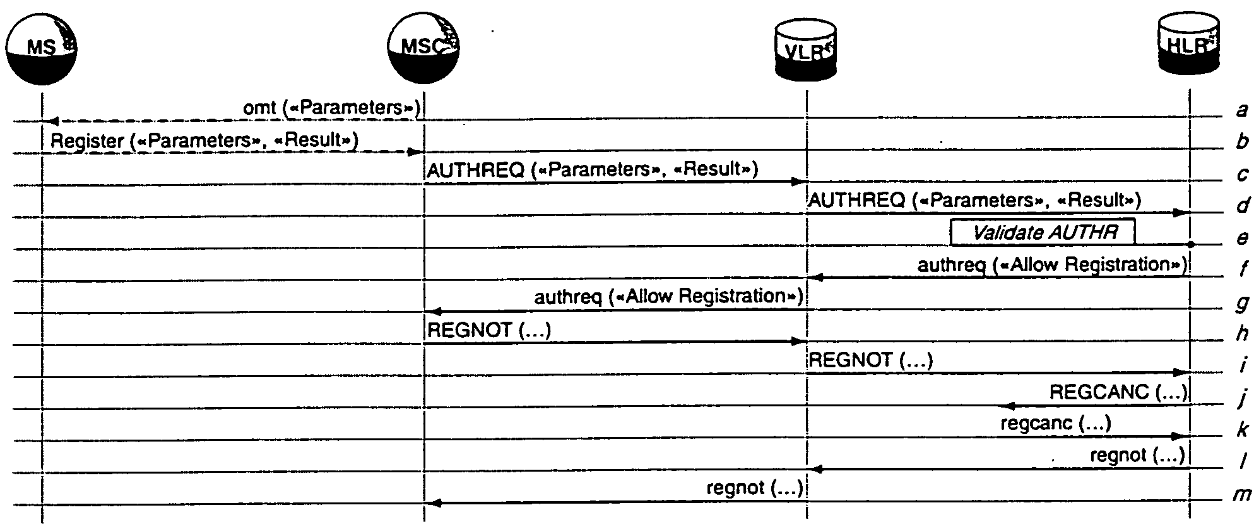
Authentication is based on cryptographic techniques to validate a mobile station. The serving market (and in some instances, the home market) supplies a set of operands to a process in the MS that provides a result. These parameters are sent to the HLR and subject to the same process and the results are compared.

Authentication relies on the fact that derivation of the authentication process is extremely difficult for a fraudulent user, even if the operands and result are known.

The following section describes a simple authentication scenario. Other scenarios are supported, but are not described here.

4.4.1 Architecture Overview

Figure 4-4. Authentication Architecture Model



a. A mobile user roams to a serving market where the Authentication feature is available. An overhead message train (omt) in the radio interface provides the parameters necessary for the MS to calculate a value based on the supplied parameters and secret data resident in the MS.

b. The MS initiates registration and supplies the calculation result.

c. An AUTHREQ message is sent from the serving MSC to the VLR containing the input parameters, except for the secret data, and the calculation result.

d. The AUTHREQ is forwarded to the HLR.

e. The HLR uses the supplied parameters and an internally stored copy of the secret data to perform the same calculation executed by the MS. It compares the result with the result sent in the AUTHREQ. If they are equal, the MS is assumed legitimate.

f. The authreq response contains an indication of successful authentication.

g. The authreq response is forwarded to the serving MSC.

h. A registration notification is sent from the MSC to the VLR.

i. The REGNOT is forwarded to the HLR.

j. The HLR cancels any prior registration by the MS in a different serving market (not shown) using a REGCANC message.

k. The prior serving market (not shown) acknowledges the registration cancellation.

l. The regnot response is sent to the current serving VLR.

m. The regnot response is forwarded to the serving MSC.

4.4.2 Implementation Requirements

Authentication is carried out using defined IS41 operations. Upgrades of IS41 capabilities in both the home and serving markets are required.

4.4.2.1 Home Market Requirements

To implement authentication in the HLR requires that the HLR implement the required set of IS41 operations for both an HLR and an AC.

In addition, the HLR must implement the administration functions that are associated with an AC for managing authentication data associated with an MS. The HLR processing workload is also increased since a result must be calculated for each AUTHREQ message.

4.4.2.2 Serving Market Requirements

Similar to the HLR, the serving market systems are required to set of IS41 operations that support authentication.

4.5 Roamer Verification & Reinstatement (RVR)

Compared to the PIN variations – SPINA, SPINI, and IPIN – and Authentication, RVR is not as well suited to HLR implementation.

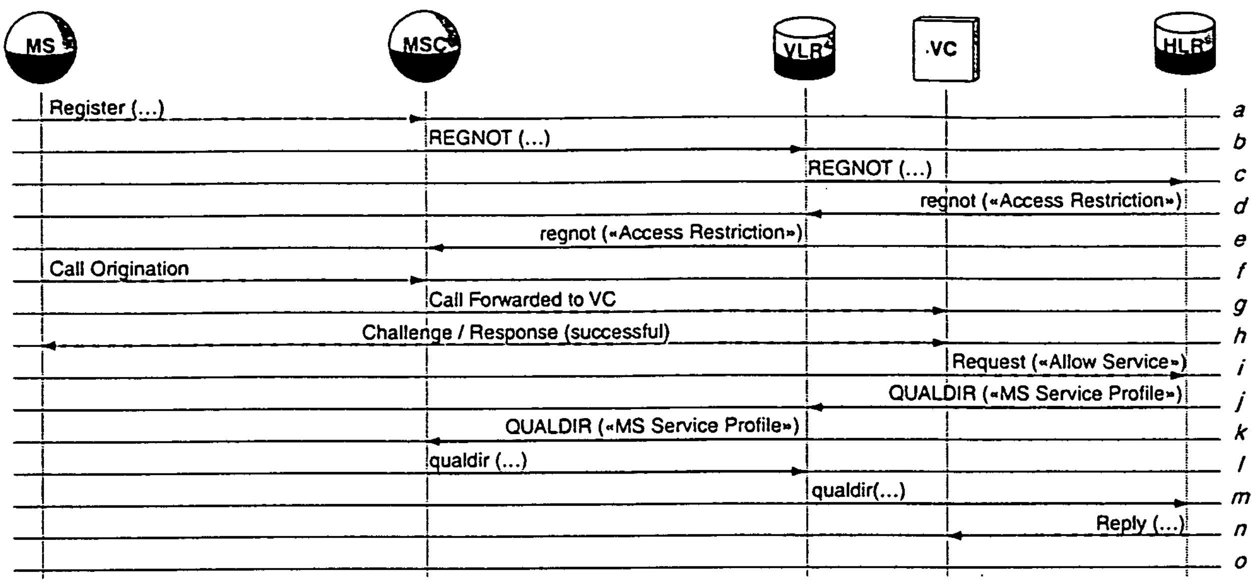
The RVR feature monitors registration events at the HLR in order to determine the status of an MS and whether or not to restrict access in the serving market. Mobile users whose access has been restricted will be routed to the RVR system If warranted the RVR system issues a verbal challenge to the mobile user in order to validate his/her identity. This challenge is made by a customer service representative, a real person, and responded to by the mobile user. The RVR system must direct calls to CSRs, which is not a function typically performed by an HLR.

RVR is driven by registration events that occur as a mobile user roams to different serving networks. It does not require per call processing.

4.5.1 Architecture Overview

RVR operation is very similar to SPINA, described previously. Registration results in an restriction on the MS, which is removed after the mobile user validates his/her identity.

Figur 4-5. RVR Architecture Mod l



a. A mobile user roams to a serving market.

b. A registration notification is sent from the MSC to the VLR.

c. The REGNOT is forwarded to the HLR.

d. The regnot response contains an access restriction on the mobile user such that calls that are originated by the mobile user will be routed to a verification center (VC).

e. The regnot response is forwarded to the serving MSC.

f. The mobile user dials a call in the normal fashion.

g. The call is forwarded to the VC and answered by a customer service representative.

h. The CSR queries the mobile user to determine if they are the legitimate user.

i. At the direction of the CSR upon a successful challenge/response, the VC issues a request to allow service in the serving market.

j. The HLR issues a QUALDIR message to the VLR with an updated profile that has the effect of removing the access restriction that were set in step d; e.g., the profile indicates that the mobile user is allowed to place and receive calls in the serving market.

k. The VLR acknowledges the QUALDIR message with a response.

l. In turn, the VLR updates the mobile user profile at the serving MSC.

m. The MSC acknowledges the QUALDIR message with a response.

n. The HLR provides an acknowledgement to the VC to indicate that the access restriction was successfully removed.

4.5.2 Implementation Requirements

4.5.2.1 Home Market Requirements

The home market must provide a verification center.

The HLR must be augmented to implement an interfaced to the verification center so that access restrictions can be placed or removed as needed.

4.5.2.2 Serving Market Requirements

There are no additional requirements that the serving market must meet in order to implement RVR.

5 A Hybrid Approach

The fraud prevention mechanisms described in the last chapter have their individual strengths and weaknesses. A hybrid approach, which takes the best characteristics of these FP defenses, is described in this section.

5.1 Integrating the Positive Traits of Conventional FP Technologies

Section 3 provided a first-order comparison among the current conventional FP mechanisms and a subjective rating of each according to the criteria of user convenience, prevention effectiveness, and cost efficiency. Profiling, RFF, RVR, and IPIN were comparably rated and tied for the lowest (best) subjective rating.

The following table lists the positive qualities of each of these technologies:

Table 5-1. Positive Traits of Conventional Approaches

FP Mechanism	Positive Qualities
Profiling	• Catalogs behavioral characteristics of a legitimate mobile user
	• Detects behaviors that are outside normal patterns for a given user
RF Fingerprinting	• Extremely user-friendly
	• Mobile user is totally unaware of RFF activity
Roamer Verification & Reinstatement	• Extremely cost-efficient
	• Cost of RVR implementation is born entirely by home service provider
Intelligent PIN	• Highly effective due to its per-call nature and the integration of profiling capability
	• Behavior aberrations are detected on a per-call basis requiring a potential cloner to provide a validation.

Borrowing and integrating the best of these mechanisms can result in a hybrid approach to fraud prevention. For convenience, the hybrid approach described here will be given Aurora's trade name for pre-call validation, PREvent®.

5.1.1 The Hybrid Result – PREvent®

The hybrid approach described here is founded first and foremost on the use of a profiling component to capture valid behaviors in the normal course of a mobile user placing (and possibly receiving) calls. It is behavior that most keenly identifies a legitimate user from an illegitimate one since they are highly unlikely to exhibit the identical behavior in using mobile telecommunications.

The hybrid approach also contains a pre-call validation component similar to IPIN, behavior that is *out-of-profile* requires the mobile user to successfully answer a challenge to their identity. Successful challenges result in an extension of the mobile user's profile to include the new behavior so that future, similar behavior is not challenged. Behavior that is clearly fraudulent as

determined by the profiling component is simply not allowed. For example, calls to *clone magnets* would be denied without asking for validation. This protects the

Like RVR, the hybrid approach can be developed and implemented predominantly by the home carrier. The events that drive the operation of this approach are IS41 MAP operations. The implementation of these operations requires the cooperation of the home and roaming market carriers. Historically, the carriers, either through cooperation or competitive pressure, have sought to establish equivalent MAP capabilities. The approach described here utilizes the current MAP operations and may be extended to include new and useful MAP operations.

Similar to RF fingerprinting, this hybrid approach is nearly, but not completely transparent to the mobile user. If the legitimate mobile user, exhibits behavior that is *in-profile*, this FP mechanism is non-intrusive.[1]

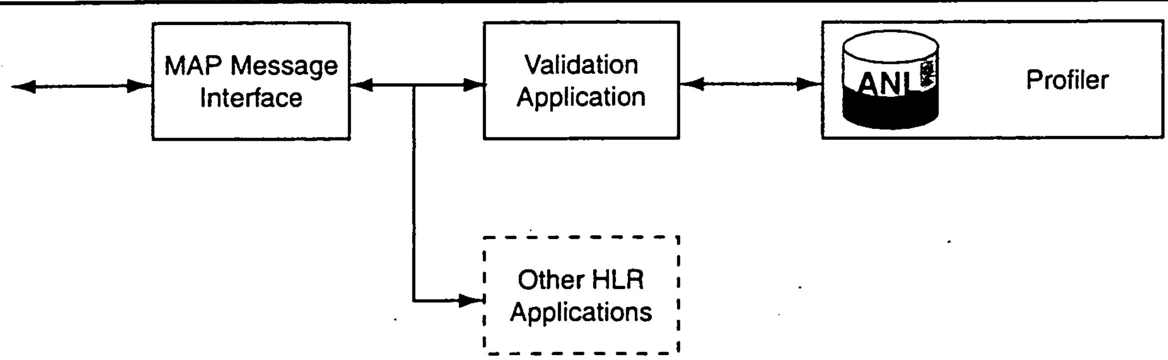
Similar to IPIN, behavior is captured, compared, and, if needed, challenged on every call attempt by a mobile user. This is what gives PREvent a high degree of effectiveness – nearly that of Authentication, but without Authentication's cost of mass handset replacement.

5.2 Architecture Overview

The hybrid approach is constructed to operate in a pre-call validation mode as illustrated in the following subsections. The goal of the operation described here is to validate the caller, if necessary, before the call attempt is allowed to complete.

The basic components required are illustrated in the following figure. The MAP message interface (MMI) provides access to the MAP commands and responses necessary to detect a service request and provide a response. The validation application, using data in the allowed number list, provides the logic to allow, deny, or validate a call attempt. Calls that are successfully validated result in an update to the allowed number list. The allowed number list is owned and managed by the profiler; hence, the profiler maintains a world view on behaviors and determines their validity.

Figure 5-1. Pre-Call Validation Component Architecture

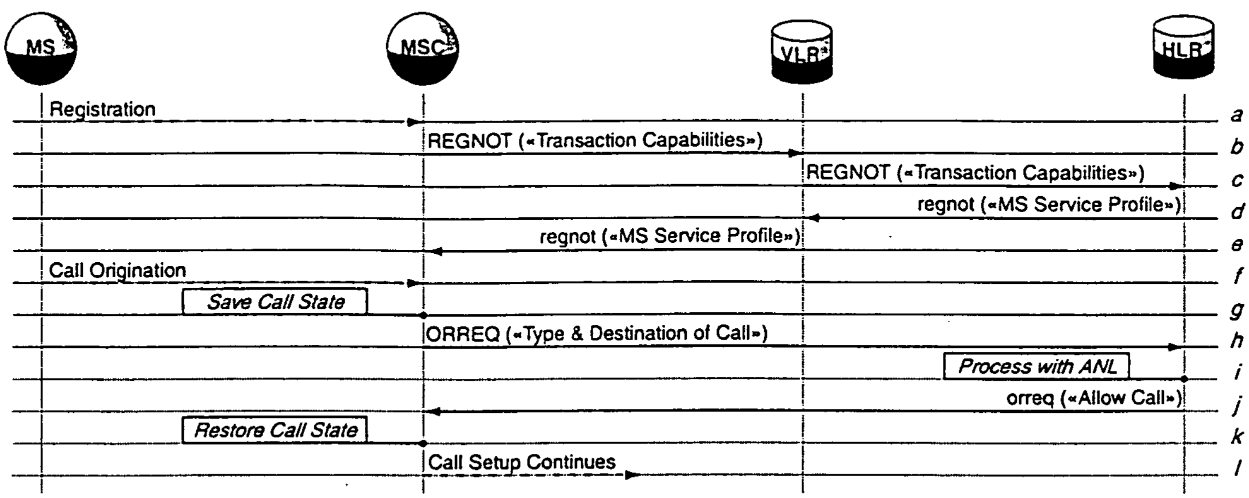


1 There is an option to operate the hybrid approach in a way so as to be completely transparent to a mobile user.

5.2.1.1 Operation for Allowed Calls

Calls that are recognized by the profiler component as clearly legitimate are simply allowed to complete without interruption or inconvenience to the mobile user. This is illustrated in the following figure and associated narrative.

Figure 5-2. PREvent Architecture Model– CallAllowed



a. A mobile user roams to a serving market where origination triggers are available.

b. A registration notification is sent from the MSC to the VLR. The REGNOT message indicates that the serving market supports origination triggers.

c. The REGNOT is forwarded to the HLR.

d. The regnot response contains a service profile for the MS that indicates the type of calls for which an ORREQ operation should be initiated. This would be set to indicate call types for which fraud is a high probability; i.e., international calls.

e. The regnot response is forwarded to the serving MSC.

f. The mobile user dials a call in the normal fashion.

g. The serving determines that an ORREQ operation is required is in effect for the MS and saves the call state.

h. The serving MSC sends an ORREQ message is sent to the HLR and indicates the type of call (e.g., local, long distance, international, etc.).

i. The HLR searches the ANL for the mobile user to determine if the called number is in the list.

j. Assuming the number is found on the ANL, an orreq response is returned to the serving MSC to indicate that the call should be allowed.

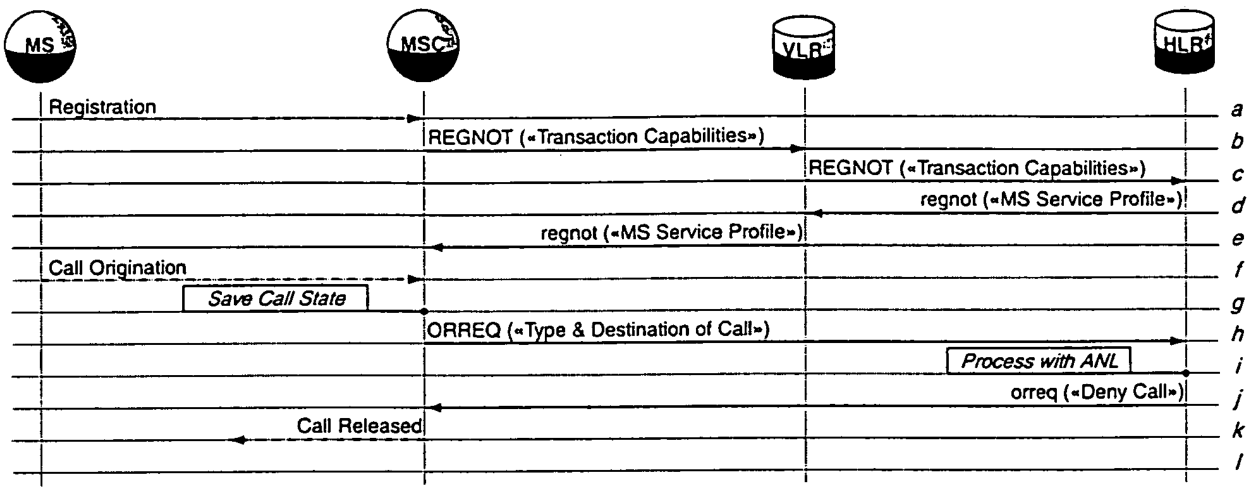
k. The serving MSC restores the saved call state.

l. Call setup continues and the call is routed to the destination dialed in step f.

5.2.1.2 Operation for D nied Calls

Calls may be recognized by the profiler component as clearly fraudulent. In this case, the call is immediately denied by the PREvent system as illustrated in the following figure and associated narrative.

Figure 5-3. PREvent Architecture Model– Call Denied



m. A mobile user roams to a serving market where origination triggers are available.

n. A registration notification is sent from the MSC to the VLR. The REGNOT message indicates that the serving market supports origination triggers.

o. The REGNOT is forwarded to the HLR.

p. The regnot response contains a service profile for the MS that indicates the type of calls for which an ORREQ operation should be initiated. This would be set to indicate call types for which fraud is a high probability; i.e., international calls.

q. The regnot response is forwarded to the serving MSC.

r. The mobile user dials a call in the normal fashion.

s. The serving determines that an ORREQ operation is required is in effect for the MS and saves the call state.

t. The serving MSC sends an ORREQ message is sent to the HLR and indicates the type of call (e.g., local, long distance, international, etc.).

u. The HLR searches the ANL for the mobile user to determine if the called number is in the list.

v. Assuming the number is on the ANL, but marked as an *always deny* number, an orreq response is returned to the serving MSC to indicate that the call should be denied.

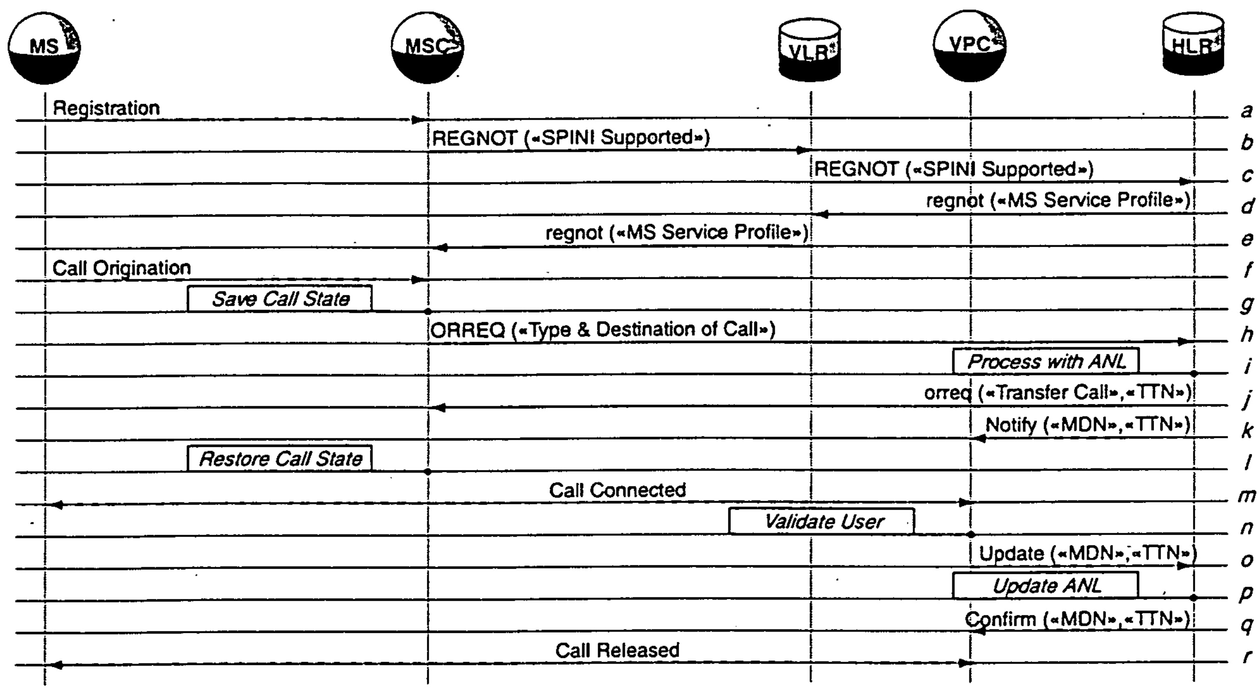
w. On receipt of the orreq response, the serving MSC releases the call.

In this scenario, the HLR also has the option of denying service to the mobile so that further call attempts are blocked within the serving market. This option might be employed if the profiling component detects known fraudulent call attempts; thus, reducing the messaging load at the HLR.

5.2.1.3 Operation for Calls Requiring Validation

Calls where the profiler is uncertain about the validity of the call attempt may require that the mobile user successfully pass a challenge; i.e., undergo validation. This moderately complex operation is described by the following figure and associated narrative.

Figure 5-4. PREvent Architecture Model– Caller Undergoes Validation



a. A mobile user roams to a serving market where origination triggers are available.

b. A registration notification is sent from the MSC to the VLR. The REGNOT message indicates that the serving market supports origination triggers.

c. The REGNOT is forwarded to the HLR.

d. The regnot response contains a service profile for the MS that indicates the type of calls for which an ORREQ operation should be initiated. This would be set to indicate call types for which fraud is a high probability; i.e., international calls.

e. The regnot response is forwarded to the serving MSC.

f. The mobile user dials a call in the normal fashion.

g. The serving determines that an ORREQ operation is required is in effect for the MS and saves the call state.

h. The serving MSC sends an ORREQ message is sent to the HLR and indicates the type of call (e.g., local, long distance, international, etc.).

i. The HLR searches the ANL for the mobile user to determine if the called number is in the list.

j. Assuming the number is not on the ANL, an orreq response is returned to the serving MSC to indicate that the call should be transferred to a validation processing center (VPC). The HLR selects a transfer-to-number (TTN) from a list of available TTNs. The TTN is associated with the MIN until the VPC issues a subsequent confirmation that the validation has occurred.[2]

k. The HLR notifies the VPC of the association of a mobile directory number (MDN) and the TTN so that the mobile user can be identified at the VPC.

l. On receipt of the orreq response, the serving MSC continues call setup.

m. The call is connected to a customer service representative at the VPC the call.

n. A challenge (question) and response (answer) sequence and, in this case, validates the mobile user as legitimate.[3]

o. The VPC directs the HLR to update the ANL for the mobile user to add the original called number to the list. Subsequent calls to this number will be allowed.

p. The HLR updates the ANL for the mobile user.

q. The HLR issues a confirmation that the update has been completed.

r. Upon receipt of confirmation, the VPC releases the call. The mobile user is instructed to retry the call, which will follow the scenario illustrated earlier for allowed calls.

As illustrated the validation operation is a moderately complex one since it requires the ability to interact with the mobile user to obtain validation information. A simplification is possible if the profiler simply declares a call to be legitimate or fraudulent. In either case, the operation defaults to the Allowed Calls or Denied Calls operation described previously.

---

2 The TTN/MDN combination can be considered a transaction identifier for a validation transaction between the VPC and the HLR

3 Other mechanisms may be used to issue the challenge respons . The VPC may utilize an automated voice response system to issue challenges or the VPC may request spoken phrases and validate the mobile user by speech recognition technology.

5.3 Implementation Requirements

5.3.1 Home Market Requirements

The HLR must be extended or designed to support an ANL for each mobile subscriber. The list typically requires on the order of 100 entries per subscriber, since the population of frequently called numbers is small. This represents an HLR database increase of Nx100x(M/2) bytes where N is the number of mobile users served by the HLR and M is the number of digits in a dialable number.[4] .

The HLR must also implement the VPC message interface that consists of the Notify, Update, and Confirm messages. This interface would probably be based TCP/IP sockets over an Ethernet physical network. If the VPC is not co-located with the HLR, then an intervening wide area network is required. In this case, multiple HLRs could be supported by a single VPC.

Both the HLR and VPC must be designed to support a work load that is proportional to the busy hour calling rate in the network that they serve. Each system is involved in the setup phase of each call; hence, they are required to add minimal delay to the call setup times, typically less than 200 milliseconds.

The home carrier must be able to efficiently administer both the HLR and VPC. This may require custom interfaces for OA&M to allow the VPC and HLR to integrate will with the support systems already present in the home carrier. Extensions to an existing HLR to implement the ANL processing will require administration extensions to maintain the ANL on behalf of a subscriber.

A web-based administration interface to the VPC may be a better approach and may not impact legacy support systems.

While the implementation has been described as though it were part of an HLR, it is possible to implement this arrangement as a system that is adjacent to, but completely separate from the HLR. Such an implementation allows deployment in existing markets where one or more HLRs may already exist.

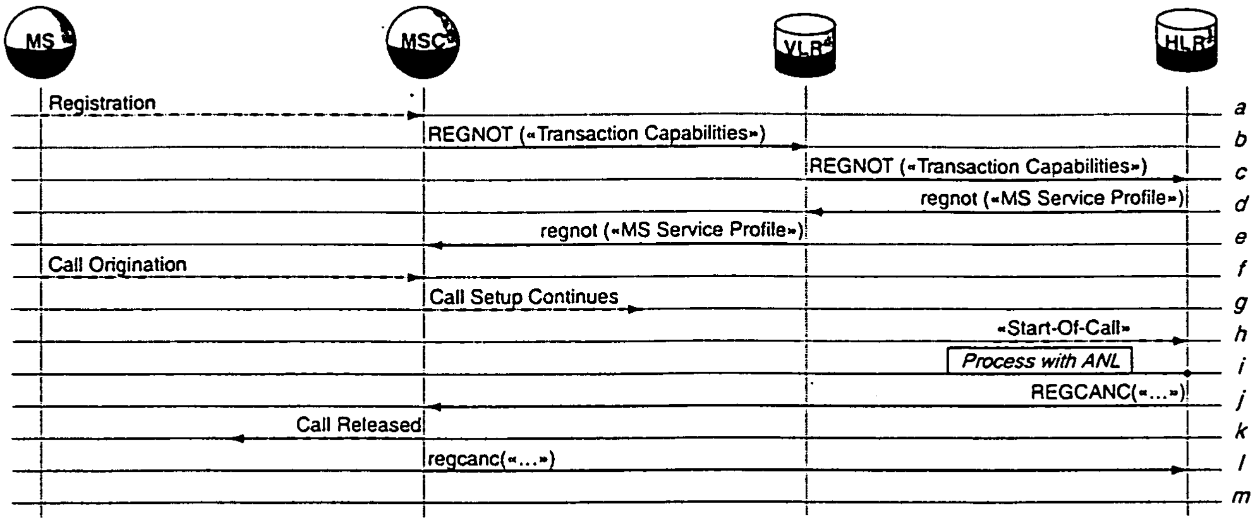
5.3.2 Serving Market Requirements

For the PREvent operation as described above, the serving market MSCs must be upgraded to IS41 Revision C, or similar, capabilities to support the ORREQ operation since it is necessary to know call information at the start of a call.

The need for the ORREQ operation can be eliminated if the profiler has access to a real-time billing data stream that provide the same type of start-of-call information -- i.e., the called and calling numbers that the profiler uses to decide whether or not the call is legitimate. This approach is illustrated in the following figure and associated narrative.

4 Each byte can store 2 binary coded decimal (BCD) digits; hence, the factor M/2.

Figure 5-5. PREvent Archit ctur Model– Caller Und rg es Validation



a. A mobile user roams to a serving market where origination triggers are available.

b. A registration notification is sent from the MSC to the VLR. The REGNOT message indicates that the serving market supports origination triggers.

c. The REGNOT is forwarded to the HLR.

d. The regnot response contains a service profile for the MS that indicates the type of calls for which an ORREQ operation should be initiated. This would be set to indicate call types for which fraud is a high probability; i.e., international calls.

e. The regnot response is forwarded to the serving MSC.

f. The mobile user dials a call in the normal fashion.

g. The serving MSC allows call setup to continue normally.

h. Some time later, the HLR receives a *start-of-call* message; e.g., from a real-time billing information stream.

i. The validation application uses this event to determine if the call is fraudulent by searching the ANL for the mobile user to determine if the called number is in the list.

j. Assuming the number is on the ANL, but marked as an *always deny* number, the HLR sends a REGCANC message to the serving MSC (via the serving VLR). This has the effect of interrupting the call in progress.

k. On receipt of the REGCANC, the serving MSC releases the call.

l. A regcanc response message is returned by the serving MSC to the HLR (via the serving VLR) to indicate completion of the requested registration cancellation.

6 Summary & Conclusions

This document presented several different fraud prevention mechanisms for use in cellular networks – profiling, PIN (with the variations of SPINA, SPINI, and IPIN), RF fingerprinting, roamer verification and reinstatement, and Authentication. Currently, RF fingerprinting, RVR, and Authentication are widely used in North American markets.

The choice of an FP mechanism is firstly based on user convenience with preference given to techniques that do not require the mobile user to learn a new way to use his/her service. Non-intrusiveness is necessary for user acceptance and customer satisfaction. Of the FP mechanisms discussed, only profiling, RF fingerprinting, and Authentication are non-intrusive.

Secondary criteria for employing an FP approach is its effectiveness at preventing fraud and its cost. Profiling is ineffective as a fraud prevention mechanism, but is useful for detection of fraud. Authentication, given its basis in cryptographic techniques, is least susceptible to compromise of all the FP mechanisms presented.

Regarding cost, solutions that offer the best return-on-investment are favored. This document has not attempted to make any determination of relative costs among the approaches presented since the expenditures for a given technique are highly variable.

Effectiveness is also determined by how well the approach is supported by a carrier's roaming partners; a solutions that does not require an inordinate amount of effort from the roaming partner is preferred. Profiling and RVR are the only two mechanisms presented that do not require any effort from a carrier's roaming partners.

An HLR may be augmented to support fraud prevention in addition to mobility management. PIN, Authentication, and RVR are all suitable, to varying degrees for implementation in an HLR. However, each in some way, falls short of an ideal solution.

Taking the best traits of current FP mechanisms, a new mechanism is proposed as the basis for the Aurora PREvent system. This approach requires the development of new HLR capabilities to interface to a validation processing complex. A VPC must be developed that utilized CSRs, automated voice response, or other validation technology.

This page is blank intentionally and is included for pagination purposes only.

Digitally signed by Mark Beckner
cn=Mark Beckner, ou=Development,
o=TecKnowledge Associates Inc., c=US
Date: 1999.11.12 00:43:18 Z
Reason: I am the author of this document
St. Charles, Illinois, USA